



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/021,450	12/13/2001	David E. Halasz	72255/13066	2167

23380 7590 01/17/2006

TUCKER, ELLIS & WEST LLP
1150 HUNTINGTON BUILDING
925 EUCLID AVENUE
CLEVELAND, OH 44115-1475

EXAMINER

POLTORAK, PIOTR

ART UNIT PAPER NUMBER

2134

DATE MAILED: 01/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/021,450

Applicant(s)

HALASZ ET AL.

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 September 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3,5-10,12,14 and 16-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3,5-10,12,14 and 16-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 September 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____

DETAILED ACTION

1. The Amendment, and remarks therein, received on 9/1/05 have been entered and carefully considered.
2. The Amendment introduces new claims 19-21 and new limitations into the originally sole independent claims 1 and 10 that has required a new search and consideration of the pending claims. The new search has resulted in newly discovered prior art. New grounds of rejection based on the newly discovered prior art follow below.
3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

4. Applicant's arguments have been carefully considered but they were not found persuasive.
5. Applicant arguments essentially contest two issues: the location of broadcast keys and a mechanism of communicating a broadcast key to the wireless station.
6. In particular applicant argues that the broadcast keys as claimed are stored at the access point and not at the authentication server as disclosed in the prior art.
7. The examiner points out that applicant's desired interpretation is not reflected by the claim limitation. Although applicant recites: "storing a table associating a broadcast key with a VLAN", this limitation stops short of requiring that the broadcast keys are store at the access point. Other limitations in claims 1 and 10 vaguely suggest that access point may (at some point) store a key (e.g. as they forward it to a client) but they do not limit the claim language to applicant's desired interpretation.

8. Also, the limitation: "wherein the access point is responsive to receiving a VLAN identifier for the wireless station to ascertain an appropriate broadcast key corresponding to the received VLAN identifier via the lookup table" in the new claim 21 does not prohibit including the authentication server in the process of ascertaining, or another words the lookup table could be stored at the authentication server.
9. However, even if the intended limitation was present in the claim language the art of record discloses this limitation as it is shown in the rejection below.
10. As per claims 19-20 and 22 applicant argues the newly introduced limitation: "a broadcast key sent to the wireless station is encrypted by the wireless station's session key" and as a result this limitation is addressed in the current Office Action, below.
11. Claims 1, 3, 5-10, 12, 14, 16-22 have been examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 1,3, 6, 8, 10, 12, 17 and 19-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Ichikawa et al.* (U.S. Patent No. 6307837) in view of *Kerberos* as

Art Unit: 2134

12. Claims 1,3, 6, 8, 10, 12, 17 and 19-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Ichikawa et al.* (U.S. Patent No. 6307837) in view of *Kerberos* as illustrated by *De Clercq et al.* (*Jan De Clercq and Micky Balladelli "Windows 2000 Authentication", March 2001, Digital Press*).

13. As per claims 21-22 *Ichikawa et al.* teach a wireless LAN (VLAN subnets, Fig. 1 and col. 7 lines 1-5). *Ichikawa et al.* teach that when starting communication, a wireless packet terminal 1-7 sends a communication startup request signal (2-1) to the wireless base station 1-6. The wireless base station 1-6 receives the communication startup request signal in the terminal authentication section 10, and sends a terminal information request (2-2) to the terminal authentication server 1-8. In response to the terminal information request, terminal authentication server 1-8 forwards terminal information notice to the wireless base station 1-6. Upon receiving the terminal information notice (2-3), terminal authentication section 10 stores the received terminal information in the terminal information memory section 11. Next, terminal authentication section 10 generates a random number for the purpose of terminal authentication and prepares an encryption of the random number using the encryption key provided in the terminal information, and the encrypted random number is sent, as the authentication request signal (2-4) to wireless packet terminal 1-7. Wireless packet terminal 1-7 decodes the encrypted random number received from the wireless base station 1-6 using the encryption key which had been pre-notified by the wireless packet network, and sends the result back to the wireless base station 1-6 as the authentication response signal (2-5). Wireless base station

1-6 compares returned random number with the random number, previously sent as the authentication request signal from the terminal authentication section 10. When the two random numbers match, terminal authentication section 10 decides that wireless packet terminal 1-7 is an authorized terminal, and so notifies the wireless packet terminal 1-7, using the authentication reception signal (2-6), that the communication is allowed (*Ichikawa et al.*, col. 7 line 49-col. 8 line 10).

14. This reads on: "a wireless access point configured to send and receive wireless signals from a wireless station and responsive to an association request from the wireless station to authenticate the wireless station with an authentication server".

15. *Ichikawa et al.* teach that when sending a broadcast or multicast packet, the wireless packet terminal 7-7 selects VLAN-key for encryption, and sends encrypted data packet (8-1) to the wireless base station 7-6. In response to such key selection, packet decoding section 13 decodes the data packet using the VLAN-key. Packet tampering detection section 14 examines whether the decoded data packet has been tampered by following the steps shown in FIG. 4, and if there is tampering, the data packet is discarded. On the other hand, if tampering is not detected, terminal address/VLAN-ID comparison section 15 confirms identity of VLAN-ID 4-3 and source address 4-2, as in Embodiment 2, and if the identity is registered in the terminal information, sends the data packet (8-2) to the destination terminal specified by the destination address (*col. 12 lines 44-61*).

16. This reads on: "the access point is responsive to receiving a VLAN identifier for the wireless station to ascertain an appropriate broadcast key corresponding to the received VLAN identifier".
17. *Ichikawa et al.* teach the access point (the wireless base station) selecting a broadcast key (*VLAN –key*) as discussed above but do not explicitly teach a lookup table containing broadcast key values corresponding to VLAN identifiers (*VLAN-id*).
18. However, *Ichikawa et al.* disclose that access point (*the wireless base station*) checks a VLAN identifier, the source address and selects an appropriate broadcast key from a group of encryption keys in order to decrypt encrypted broadcast data from the wireless station (*col. 10 lines 42-46, col. 12 lines 44-54, col. 13 lines 12-15*). Thus, it is clear that the access point must have a lookup table like structure similar to lookup table 1 (*col. 8*) in order to retrieve the information discussed above.
19. *Ichikawa et al.* do not explicitly teach that an authentication server sends a session key to the wireless station.
20. *Kerberos* use the authentication server that provides session keys to network clients (*Key Distribution Center (KDC), e.g. The introduction, "Step 1: Kerberos authentication is based on symmetric key cryptography" section and Fig. 9*)
21. As well known in the art session keys provide means for secure communication where data exchanged between the communicating parties is encrypted. Also, session keys are valid only for the particular session and compromising a session key does not impact the security of the previous and the future data exchange. Furthermore, *Kerberos* provides scalability and ensure central administration, which

is particularly beneficial since the network clients are often installed and kept in an unsecured environment. Given these benefits it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use centralized authentication server to provide session keys to a network client such as wireless workstation taught by *Ichikawa et al.*

22. The examiner points out that the wireless stations are connected to the network via access points thus any data sent to the wireless station will be received by the appropriate access point that then sends data to the wireless station.

23. *Ichikawa et al.* do not explicitly teach encrypting the broadcast key with the session key. However, the limitation is implicit. The broadcast key is to encrypt broadcast data in order to protect the data confidentiality. Sending the broadcast key unencrypted defeats the purpose of the security since obtaining the "unprotected broadcast key" jeopardize the confidentiality of the encrypted broadcast data.

24. Claims 1,3, 6, 8, 10, 12, 17 and 19-20 are substantially equivalent to claims 21-22; therefore claim 1,3, 6, 8, 10, 12, 17 and 19-20 are similarly rejected.

25. As per claims 8 and 17 *Ichikawa et al.* teach the network using an IP address scheme (*col. 21 lines 37-52 and col. 24 lines 33-36*).

26. Claims 5 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Ichikawa et al.* (U.S. Patent No. 6307837) in view of in view of *Kerberos* as illustrated by *De Clercq et al.* (*Jan De Clercq and Micky Balladelli "Windows 2000 Authentication", March 2001, Digital Press*) in further in view of *Johnson et al.* (U.S. Pub. No. 20010014088).

27. *Ichikawa et al.* in view of *Kerberos* teach a wireless station as discussed above.

Ichikawa et al. in view of *Kerberos* do not explicitly teach that the wireless station operates in accordance with the IEEE 802.11 standard.

Johnson et al. teach wireless stations operating in accordance with the IEEE 802.11 standard (*Johnson et al.*, col. 1 lines [4]).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to operate *Ichikawa et al.* in view of *Kerberos*' wireless stations in accordance with the IEEE 802.11 as taught by *Johnson et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to minimize data packet collisions.

28. Claims 7, 9, 16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Ichikawa et al.* (U.S. Patent No. 6307837) in view of in view of *Kerberos* as illustrated by *De Clercq et al.* (*Jan De Clercq and Micky Balladelli "Windows 2000 Authentication", March 2001, Digital Press*) in further in view of *Ke et al.* (U.S. Pub. No. 20030041266).

29. *Ichikawa et al.* in view of *Kerberos* teach a mobile IP VLANs as discussed above.

Ichikawa et al. in view of *Kerberos* do not explicitly teach a step of tagging data to which VLAN the data belongs.

Ke et al. teach tagging (*Ke et al.* [34]).

30. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to tag data to which VLAN the data belongs as taught by *Ke et al.* One of

ordinary skill in the art would have been motivated to perform such a modification in order to allow traffic to be mapped into a particular VLAN (*Ke et al. [34]*).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

Art Unit: 2134

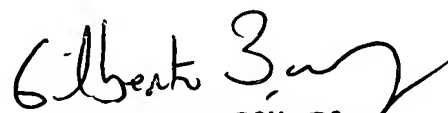
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Signature

12/29/05

Date


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100